FANS
SAS Cloud after SCHREMS II
Now fully compliant

Jonas Lie-Nielsen

09/02-23

What SAS Customers in Nordics runs Viya4 in SAS Cloud

All signed last year

- Sparebanken Sør
- DNB
- Conoco Philips
- Posten
- Nordea
- Arbeidernes Landsbank
- Scania

Before Schrems II, SAS maintained two overlapping protections for EU-US transfers, involving a privacy certification and privacy-related contract terms

EU-US Privacy Shield

The EU-US Privacy Shield is a legal framework a non-EU company commits to for data transfers between the EU and US.

SAS is EU-US Privacy Shield certified

Standard Contractual Clauses (SCCs)

Standard Contractual Clauses (SCCs) are agreements between the EU company (data controllers) and the IT service provider (data processors).

Many of SAS' EU Customers already requested the execution of SCCs in addition to the EU-US Privacy Shield certification

The SCHREMS cases questioned requirements for protection of EU data transfers to the US, involving data storage, processing and access

Max Schrems is a young lawyer from Austria who brought legal challenges against Facebook's mechanisms for transferring data from the EU to the US (Schrems I and Schrems II)

These challenges were finally decided by the Court of Justice of the European Union (CJEU)

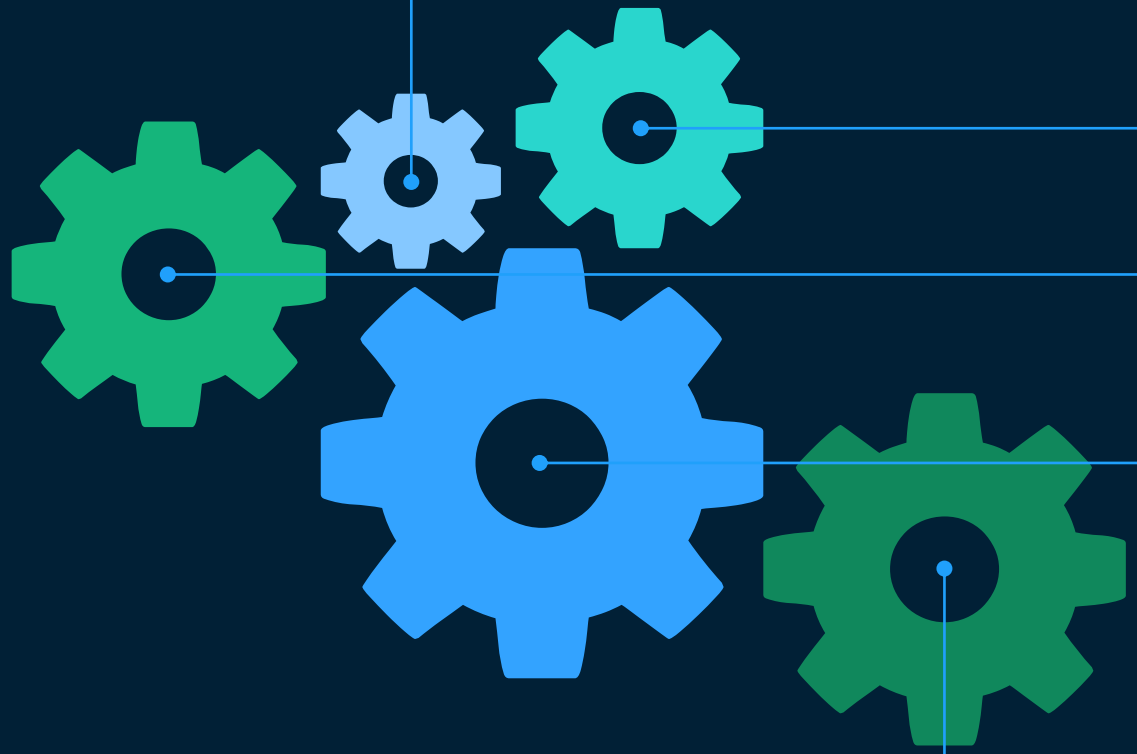
In the Schrems II case, Mr. Schrems alleged that Facebook's use of Standard Contractual Clauses (SCCs) to transfer data from Europe to Facebook Inc. in the US does not ensure an adequate level of protection for EU data subjects

CJEU declared the European Commission's Privacy Shield (adequacy) Decision invalid and stipulated stricter requirements for the transfer of personal data based on standard contract clauses (SCCs)
- both on account of US surveillance programmes.

The result of Schrems II culminated in the requirement for data controllers to perform impact assessments, which ensure that adequate controls are in place

- In June 2021, the EU Commission released updated SCCs – mandatory for new agreements as of SEPT 27, 2021, for existing agreements new SCCs need to be amended until DEC 27, 2022
- Exporter needs to do a "Transfer Impact Assessment" or "TIA" to determine whether the transferred personal data can be protected from inappropriate access by law enforcement and national security authorities in the inadequate jurisdiction.
- In addition to SCCs controllers (customers) must assess on a case-by-case basis whether supplementary measures need to be implemented in order to bring the level of protection of the transferred data up to the EU standard of essential equivalence
- European Data Protection Board (EDPB) published guidelines on international data transfers

SAS Customers, as data controllers, perform these impact assessments on a case-by-case basis



Transfer Impact Assessment – customer responsibility

Additional Technical Measures

Contractual Commitments including new SCCs

Data Location at Rest and in Transit

Additional Organizational Measures

SAS' Response to SCHREMS supports our customers in conducting their impact/risk assessments as well as assessing supplemental controls

Supplementary measures and response to surveillance

SAS is fully up to date to latest SCC

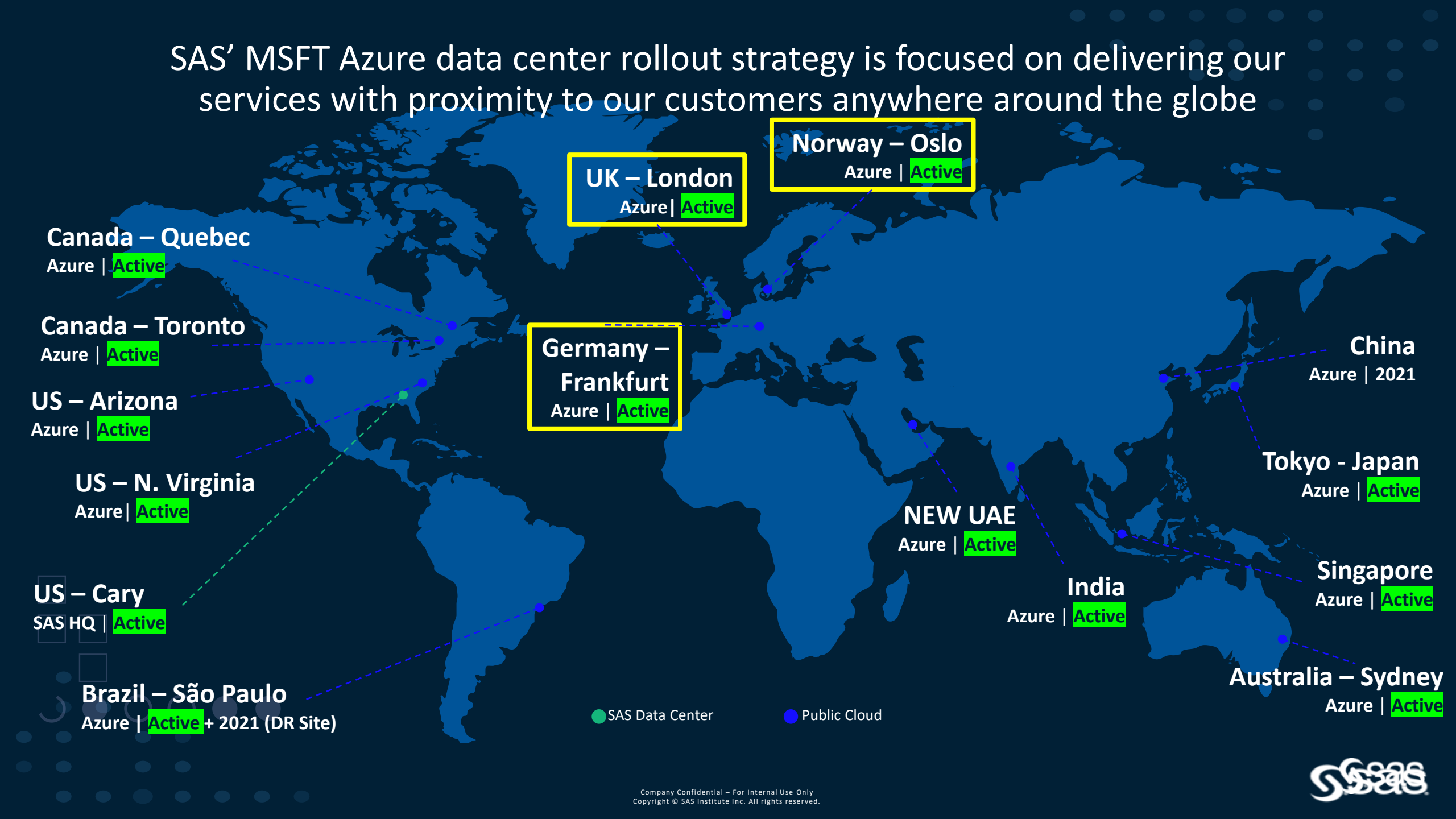
- Low Risk of Government Access Request
  - SCC of June 2021 open for taking into account how US laws are applied in practice
  - SAS has never received a government request from a law enforcement authority or state security body
  - Companies at risk is the public communication carriers - As the U.S. government has applied FISA § 702, it uses upstream orders only to target traffic flowing through internet backbone providers that carry Internet traffic for third parties (i.e., telecommunications carriers
- Supplemental measures
  - Contractual measures: SAS agrees to be bound by the SCCs – e.g. agreement of data processing within UK /EU
  - Organizational measures
    - All requests must be forwarded to SAS Legal
    - SAS will challenge the request to the fullest extend possible using internal and external resources
  - Transparency: SAS commits to publishing annual transparency report of government requests

Trust Center | SAS

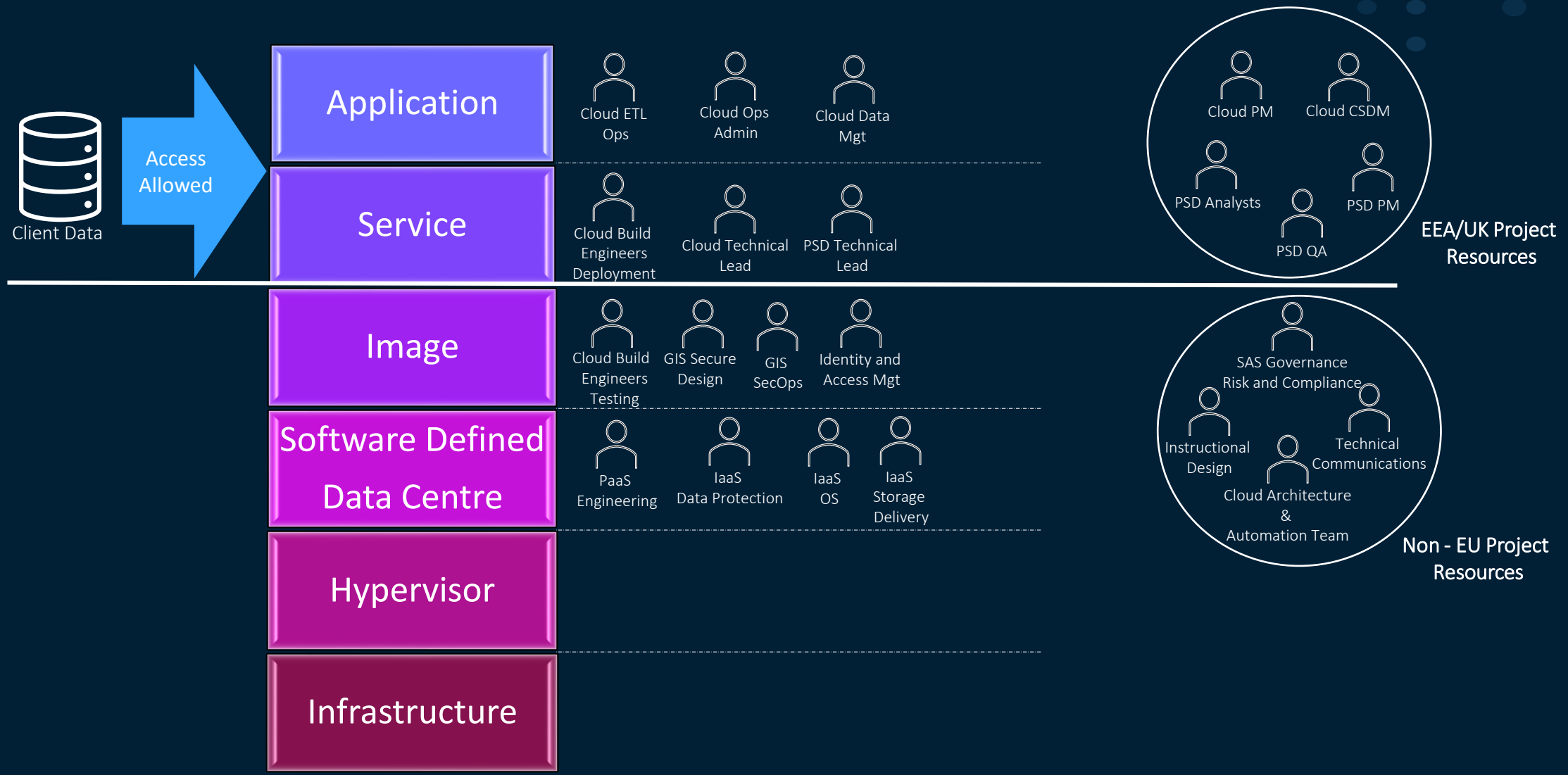
Technical measurements

- Microsoft garantees that the data is not outside of Norway and that they operate Schrems II compliant
- Following security standards ISO 27001, ISO27017 and ISO27018, with SOC 2, and SOC 3
- SAS security and quality process SAS Product Quality Whitepaper
- Encryption of data at rest and in-motion
- Role Based Access Control / Privileged Access Management (PAM)
- EU specific admin accounts
- SAS Admins using customer accounts to log-on to Viya – full visibility
- All operations done within EU/UK 24*7

SAS' MSFT Azure data center rollout strategy is focused on delivering our services with proximity to our customers anywhere around the globe

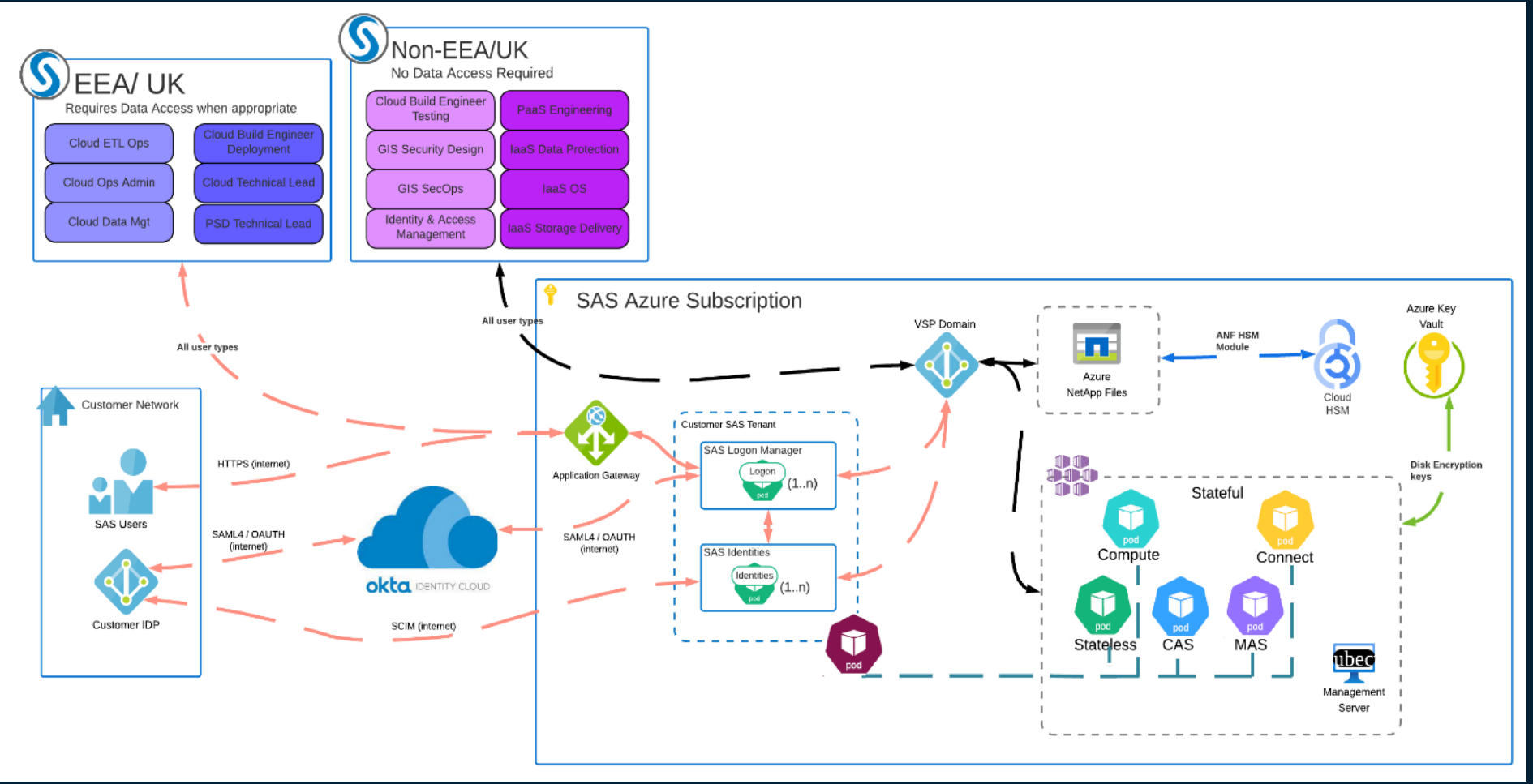


Role Based Access Control - Diagram



Authentication of SAS employees

Split between front and back door access



FAQ

- Can personal data be transferred using SSC?
  - SCCs still remain a valid, legal mechanism for data transfers, although exporter needs to do a risk assessment on a case-by-case basis.
- Can other resources access the environments?
  - Access could be granted in the event of an issue that requires R&D. Such access will be requested when needed and must be approved by the client.
- Will CIS resources be able to access the environments during build?
  - CIS and SAS Cloud build resources will have access to the environment to ensure the build and quality of the environment. As client data is migrated / loaded the environment will be locked down to EU resources.
- Can UK resources support EU clients?
  - Yes. The UK were given an Adequacy Decision (same level of data protection) for data transfers.
- How do SAS Cloud and CIS resources know the client has data restrictions?
  - As part of the Customer Relationship record (CREL), each client will have a security restriction category added. This is checked prior to any work carried out. Should a restriction be seen, they would triage to the correct team.
- Who controls access to the HMS and RMS Environments?
  - For HMS access is controlled by SAS, unless SSO services are included in the service. SSO is then controlled by the Client IAM team. RMS access is fully within the control of the Client.
- Why do we need a data processing agreement when no one from SAS is processing client data during Customer's business operations?
  - The definition of processing is very broad, any use, any kind of "making available", remote access, even reading is deemed processing. For many authorities just the possibility of access is sufficient.
- If the Personal Data is stored in an EU data center why should we care about a transfer to the US or other third countries?
  - the term "transfer" is typically understood to mean sending data to a recipient, with the intent that the recipient will receive and store a copy of the data in its own facilities or systems. Under GDPR, a "transfer" can also occur when an organization merely makes data accessible to an external party, even if the data is only viewed remotely and is not stored on the external party's systems.